records the message or the subscriber activates a plug-in of the browser **144** to record the message (voice, video, text, etc.). Using the application, the subscriber edits, rerecords, etc. the message until satisfied. When finished the user provides a file name to the recording and stores it locally. The browser **144** is then used to POST the message to the server. Alternatively, the browser **144** can be used to request that the server **146** record the message and send it. The server responds by performing the steps **1–21** for refreshing a page previously discussed and forwards a template for a page, such as depicted in FIG. **11**. The subscriber completes the template by providing the file name of the recording, addresses (such as telephone numbers, e-mail addresses, etc.) of the recipient along with indicators for privacy, etc. The browser **144** when the "submit message" button is pressed creates a message header, attaches the file and sends the file to the server **146**. The server **146**, when the file appears in the incoming message directory, converts the message into an appropriate storage format (compresses it if necessary) and stores the message. The header is reviewed to ascertain the recipient addresses and the message is retrieved and sent to the recipients. For example, a voice message to a particular telephone number would result in an outdial process being performed. If the recipient is a subscriber the message is copied to the recipients mailbox.

The present invention enhances the security of each session with a number of different features.

Unit **126** is preferably limited to the HTTP (Hypertext Transfer Protocol) and SSL (Secure Sockets Layer) type Internet service to help eliminate problems associated with unsecure protocols. The present invention also has certain authentication features. A request is first sent from the browser **144** to the server **146** that does not include authentication. The Microsoft Internet Information Server (IIS-**170**) software running in the server **146** checks this request. The filter **170** also checks to see if the user is valid and since there is no authentication the check fails and the browser **144** sends the request again this time with authentication. The request either passes or fails based on the authentication. When the request fails the browser **144** is notified. When the request passes the request is forwarded for processing. In an initial log-in situation the request is forwarded to the users home APU **150** where the validity of the user is checked again to determine whether the user is a subscriber. This double validation helps prevent nonsubscribers from obtaining access to the system. When the user is a subscriber the user gets a message list sent to the browser **144** where it is displayed. Once a session is established the user is essentially communicating with the home APU **150** for this subscriber which controls further transactions. All further requests by the browser **144** to the server **146** go through the first level of authentication.

The system preferably uses secure socket layer (SSL) packet encryption.

The present invention also is preferably implemented using dual homed-host Internet processing units that prevents packet sniffing on the internal ethernet. A dual homed-host is a host that has two IP addresses that correspond to one or more physical addresses allowing it to be configured differently based on the IP address. For example, one IP could be configured only to work with SSL active and the other IP is used in the clear, i.e. without SSL.

The provision of a router to perform packet filtering prevents source address spoofing.

The present invention also assigns session numbers and specifically created file names to files that are transferred to the browser **44**. In this filter operation the process removes all correlation to any data set internal to the platform **132** from data sent over the network **136**. For example, a message identifier that is sent to the browser includes a session identifier and a randomly assigned file identifier (which can be the current time of day). The server **146** creates a session information entry that identifies the file for the session identifier and the randomly assigned file identifier. When the browser **144** requests the file the session identifier and previously assigned file identifier are included with the request. The server **146** uses the session information to convert the file name into a real file name to retrieve the file. When the server **146** sends the requested file to the browser **144** the server **146**, if it is not a streamed data file, the server **146** assigns a pseudo file name that includes a session number and a randomly created file name. This pseudo file name and the real file name are also stored in the session information so that the file can be requested again. The session number is part of the create identifier to allow communications that use the same random number to be distinguished. If the file is a streamed data file, the data of the file with content type is sent without any file name identification.

The present invention preferably uses a buffer of 8192 bytes to improve transfer efficiency even though a buffer size of from 512 bytes to 8192, except for 4096 for certain audio formats when the data is audio, will work.

The present invention, through the network interface provides two methods of message deletion: immediate or marking messages to be deleted with a deletion "Commit" (see FIG. **8**) at the end of a session. The second option is like the deletion feature of the audio (telephone) interface where messages to be deleted can be listened to again thereby removing the delete flag and only those messages flagged for deletion are deleted when the audio session is ended.

The present invention also allows different types of messages to be bundled together into a multimedia type message with multiple body parts. The state information for a message includes body part information which indicates the content type of the body part.

The present invention is also suitable for providing electronic data interchange (EDI) services where EDI forms, such as purchase order forms, are provided to a user for the purchase of goods, etc. Other types of data such as weather data can also be stored and transmitted.

The present invention, using the administration features, can be configured through the network interface to perform operations such as sending standard text or voice messages to doctor's patients.

The administration of mailbox features, such as the password, telephone ring count, etc., is performed using HTML templates that can be customized for each service provider.

The present invention provides priority of access to a mailbox by one of the owners to accesses that are made through the telephone interface.

The browser **144**, if it automatically requests a refresh of a currently displayed page, allows a page to be created that includes a message list icon that can be updated to reflect that a new message has arrived during the session.

The present invention also includes an automatic log-off feature that will log a subscriber out of the system when there has been no activity for a period of time. This allows subscribers to inadvertently leave their PC logged in to the system, such as when going home from work, and prevent others from accessing the system during the absence.

The administration features of the system allows a verified system administrator to access a system administration